Лабораторная работа № 3

МЕТОДЫ АДРЕСАЦИИ И ПРОТОКОЛЫ РАЗРЕШЕНИЯ АДРЕСОВ

Цель работы

Изучить методы адресации узлов, используемые в компьютерных сетях.

Изучить методы разрешения имен в ОС Windows, компоненты и инфраструктуру системы DNS.

Постановка задачи

1. Изучить основные теоретические вопросы, используя материалы лекций, рекомендуемую литературу и методические указания к лабораторной работе:
   - методы адресации узлов сети;
   - физические адреса;
   - протоколы разрешения адресов;
   - доменная система имен;
   - методы разрешения имен в ОС Windows.
2. Выполнить задания по лабораторной работе согласно вариантам.
3. Ответить на контрольные вопросы.
4. Подготовить отчет по лабораторной работе.

Методические указания

1. Методы адресации узлов сети

Каждый узел сети должен иметь адрес, чтобы была возможной передача информации и функционирование сети.

К адресу узла сети и схеме его назначения можно предъявить несколько требований:

- Адрес должен уникально идентифицировать компьютер в сети любого масштаба.
- Схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов.
- Адрес должен иметь иерархическую структуру, удобную для построения больших сетей. В крупных сетях отсутствие иерархии адресов может привести к большим издержкам - конечным узлам и коммуникационному оборудованию придется оперировать с таблицами адресов, состоящими из тысяч записей.
- Адрес должен быть удобен для пользователей сети, т.е. должен иметь символьное представление.
- Адрес должен иметь по возможности компактное представление, чтобы не перегружать память коммуникационной аппаратуры - сетевых адаптеров, маршрутизаторов и т. п.

Перечисленные требования трудно совместить в рамках какой-либо одной схемы адресации, поэтому на практике обычно используется сразу несколько схем, так что компьютер одновременно имеет несколько адресов. Каждый адрес используется в той ситуации, когда соответствующий вид адресации наиболее удобен.

Множество всех адресов, которые являются допустимыми в рамках некоторой схемы адресации, называется ***адресным пространством***. Адресное пространство может иметь ***плоскую (линейную)*** или ***иерархическую*** организацию. При плоской организации множество адресов никак не структурировано. При иерархической организации адресное пространство организовано в виде вложенных друг в друга подгрупп.

Наибольшее распространение получили **три схемы адресации узлов** (три типа адресов):

- локальные адреса;
- числовые составные адреса;
- символьные адреса или имена.

2. Протоколы разрешения адресов. Протокол ARP

Для преобразования адресов из одного вида в другой используются специальные протоколы, которые называют ***протоколами разрешения адресов*.**

Проблема установления соответствия между адресами различных типов может решаться централизованными или распределенными средствами. В случае централизованного подхода в сети выделяется один компьютер (сервер имен), в котором хранится таблица соответствия друг другу имен различных типов, например символьных имен и числовых номеров. Все остальные компьютеры обращаются к серверу имен, чтобы по символьному имени найти числовой номер компьютера, с которым необходимо обменяться данными.

При распределенном подходе, каждый компьютер сам решает задачу установления соответствия между именами. Недостатком распределенного подхода является необходимость рассылки широковещательных сообщений - такие сообщения перегружают сеть, так как они требуют обязательной обработки всеми узлами, а не только узлом назначения. Поэтому распределенный подход используется только в небольших локальных сетях. Для крупных сетей характерен централизованный подход.

Наиболее известной службой централизованного разрешения имен является служба **DNS (Domain Name System)** сети Internet.

Пример использования распределенного подхода – протокол разрешения адресов **ARP (Address Resolution Protocol),** используемый стеком TCP/IP для преобразования IP-адреса в аппаратный адрес.

Необходимость обращения к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet.

Работа протокола ARP начинается с просмотра ARP-таблицы. По таблице определяется нужный MAC-адрес. Для каждой сети, подключенной к сетевому адаптеру компьютера или порту маршрутизатора, строится отдельная ARP-таблица.

Пример.

IP-адрес	MAC-адрес	Тип записи
194.85.135.75	00-80-48-EB-7E-60	динамический
194.85.135.70	08-00-5A-21-A7-22	динамический
194.85.60.21	00-80-48-EB-75-67	статический

Работа с таблицей осуществляется с помощью специальной утилиты arp. Таблица выводится на экран по команде arp –a.

Статические записи создаются вручную с помощью утилиты arp. Они находятся в кэше до перезагрузки компьютера.

Динамические записи создаются протоколом ARP, добавляются и удаляются автоматически.

Если запись в течение определенного времени не обновляется, то она исключается из таблицы. Т.о. ARP-таблица содержит записи только об узлах, активно участвующих в сетевых операциях. Поэтому ее еще называют **ARP-кэш.**

Если искомого адреса в таблице нет, то протокол ARP широковещательно рассылает **ARP-запрос**, указывая IP-адрес («Чей это IP-адрес и каков ваш адрес сетевого адаптера?»). Узел, IP-адрес которого совпал с указанным в запросе, отправляет **ARP-ответ** с указанием

своего локального адреса на машину, сделавшую запрос. После этого новая запись добавляется в ARP-таблицу.

Если в сети нет узла с искомым IP-адресом, ARP-ответа не будет. Протокол IP уничтожает пакеты, направленные по этому адресу.

3. Одноадресные, групповые и многоадресные типы адресов

По количеству адресуемых сетевых интерфейсов адреса можно классифицировать следующим образом:

- ***Одноадресный тип*** или ***уникальный адрес (unicast)*** используется для идентификации отдельных интерфейсов (физический интерфейс между компьютером и сетью) конечного узла или маршрутизатора; позволяет пересылать сообщения в одну точку (на один конечный узел сети).

- ***Групповой адрес (multicast)*** идентифицирует сразу несколько интерфейсов, данные доставляются каждому из интерфейсов, входящих в группу; позволяет пересылать сообщения группе произвольно расположенных в Internet узлов.

- ***Широковещательный адрес (broadcast)*** используется для доставки данных всем узлам подсети;

- ***Адрес произвольной рассылки (anycast)*** задает группу интерфейсов, но данные должны быть доставлены не всем, а одному члену группы, как правило, «ближайшему» (новый тип адреса, определен в протоколе IPv6). Назначается только интерфейсам маршрутизатора.

4. Аппаратные адреса

Аппаратные адреса называют еще ***физическими*** или ***локальными***.

Локальный адрес – такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной сети. В разных подсетях допустимы различные сетевые технологии, следовательно, различные протоколы. Поэтому существуют разные типы локальных адресов. Для ЛВС локальный адрес – это MAC-адрес сетевого адаптера (Media Access Control). Если подсетью является глобальная сеть (например, протокол IP работает над IPX или X.25), то в этом случае локальными адресами будут адреса X.25 или IPX.

Физические адреса не имеют иерархической структуры, используются аппаратурой. Компьютер может иметь несколько сетевых интерфейсов и соответственно несколько физических адресов.

Записывается адрес сетевого адаптера в ПЗУ платы сетевого адаптера на заводе изготовителе. При замене сетевого адаптера изменяется и аппаратный адрес интерфейса.

Стандарты на аппаратные адреса были разработаны IEEE. Был выбран 48-битный формат адреса для всех технологий ЛВС.

Аппаратный адрес принято записывать в 16-ричном виде, разделяя байты с помощью “-“. Например: 11-AO-17-3D-BC-01 - MAC-адрес сетевого адаптера Ethernet.

Чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса:

I/G	U/L	Идентификатор производителя (22 бита)	Уникальный адрес производителя (24 бита)

Два старших разряда определяют тип адреса и способ интерпретации остальных 46 бит.

- I/G(Individual /Group) - определяет, индивидуальный это адрес или групповой:
  0 - индивидуальный;
  1 - групповой (такие пакеты получают все сетевые адаптеры с этим адресом).
- U/L (Universal /Local) – флаг определяет, как был присвоен адрес данному адаптеру:
  0 - производителем;
  1 - организацией, использующей данную сеть (редко).
- 22 разряда - Идентификатор производителя. IEEE присваивает один или несколько уникальных идентификаторов каждому производителю. Это позволяет исключить совпадения адресов адаптеров от разных производителей.(~ 4 млн. вариантов)
- Младшие 24 разряда присваивает производитель сетевого адаптера (возможно 16 млн. комбинаций).

5. Символьные адреса.

5.1 Методы разрешения имен в ОС Windows.

Символьные адреса **или** ***имена*** предназначены для запоминания людьми и поэтому обычно несут смысловую нагрузку. Символьные адреса легко использовать как в небольших, так и крупных сетях. Для работы в больших сетях символьное имя может иметь сложную иерархическую структуру.

Примеры символьных адресов – DNS и URI-адреса, имена NetBIOS.

Разрешение имен – процесс преобразования компьютерных имен в сетевые адреса.

Сети Windows Server 2008 включают три системы разрешения имен: DNS, LLMNR (Link Local Multicast Name Resolution) и NetBIOS. Основной является DNS, поскольку этот метод разрешения имен используется для поддержки служб доменов Active Directory (Active Directory Domain Services) и разрешения всех имен Интернета. Инфраструктура DNS требует настройки сетевой конфигурации на серверах и клиентах. В небольших сетях и рабочих группах используются другие службы разрешения имен — LLMNR и NetBIOS.

4.1.1 Протокол LLMNR

Метод разрешения имен Link Local Multicast Name Resolution (LLMNR) используется функцией Сетевое обнаружение (Network Discovery), которую можно включить в Центре управления сетями и общим доступом.

Преимущества протокола LLMNR:

- не требует конфигурирования;
- совместим с IPv6;
- простой, компактный.

Недостатки LLMNR:

-может применяться только в системах Windows Vista и Windows Server 2008; не разрешает имена компьютеров с предыдущими версиями Windows;

- не поддерживает IPv4;
- не работает по умолчанию, для его использования должно быть включено Сетевое обнаружение;
- нельзя использовать для разрешения имен компьютеров за пределами локальной подсети, так как для разрешения имен LLMNR использует широковещательные запросы на multicast-адрес FF02::1:3 (все IPv6-узлы сети с включенным сетевым обнаружением прослушивают трафик, пересылаемый на этот адрес).

LLMNR можно отключить одновременно для большого числа компьютеров с помощью групповой политики.

4.1.2 NetBIOS

Протокол NetBIOS обеспечивает разрешение имен в IPv4-сетях Windows без DNS. Например, в домашней беспроводной сети можно подключаться к другим компьютерам, указывая их UNC-имена (\\Имя_компьютера\Путь\Имя_файла).

NetBIOS включает три метода разрешения имен: широковещание, WINS-сервер и файл Lmhosts.

■ **Широковещание NetBIOS**. Компьютер, которому требуется разрешить имя, выполняет широковещательный запрос IPv4-адреса в локальной подсети.

■ **WINS-сервер** содержит имена компьютеров и соответствующие им IPv4-адреса. Адрес WINS-сервера надо настроить в сетевом подключении. WINS-сервер включает разрешение имен NetBIOS за пределами локальной подсети.

■ **Файл Lmhosts**. Статический файл локальной базы данных, который хранится в папке %SystemRoot%\System32\Drivers\Etc и содержит имена NetBIOSи соответствующие им IP-адреса. Файл Lmhosts требуется создать вручную. Он обычно используется, когда в сети нет WINS-сервера или когда клиентский компьютер расположен за пределами широковещательного домена.

Включение и отключение NetBIOS.

Протокол NetBIOS включен по умолчанию. Чтобы изменить параметры NetBIOS, можно открыть свойства подключения по локальной сети, затем свойства протокола Интернета версии 4 (TCP/IPv4), кнопку Дополнительно (Advanced), диалоговое окно Дополнительные параметры TCP/IP (Advanced TCP/ IP Settings), вкладку Служба WINS.

Типы узлов NetBIOS:

■ **Широковещательный (b-узел)** Использует широковещательные запросы для регистрации и разрешения имен.

■ **Узел точка-точка (p-узел)** Использует WINS-сервер для разрешения имен.

■ **Комбинированный (m-узел)** Вначале использует широковещание (b-узел), а затем, если имя не было разрешено с помощью широковещания, применяет WINS-сервер (p-узел).

■ **Смешанный (h-узел)** Вначале использует WINS-сервер (p-узел), а затем, если сервер имен недоступен,—файл Lmhosts и широковещание (b-узел).

По умолчанию клиенты Windows конфигурируются с m или h-узлом. Текущее состояние узла, назначенного компьютеру, можно определить с помощью команды Ipconfig /all (значение поля Тип узла).

Преимущества NetBIOS:

- не требует конфигурирования , включен по умолчанию;
- поддерживается всеми версиями Windows;
- при добавлении WINS-сервера NetBIOS можно использовать (аналогично DNS и в отличие от LLMNR) для разрешения имен в соседних подсетях;
- конфигурировать и управлять NetBIOS легче, чем DNS.

Недостатки NetBIOS:

- неэффективен в больших сетях;
- имя каждого компьютера должно быть уникальным для всей сети (если есть подсети);
- несовместим с IPv6-сетями;
- низкий уровень безопасности (разглашает информацию о сетевых службах).

5.2 Система DNS

Самый первый механизм назначения IP-адресам имен, удобных для человека, назывался **таблицей хостов**. (Использовался еще в сети ARPANET). Таблица хостов представляла собой обычный **текстовый файл hosts.txt** в формате ASCII, содержащий список IP-адресов и эквивалентных им хост-имен.

В наши дни таблица хостов по-прежнему сохраняется в TCP/IP системах в файле Hosts на локальном диске. Однако, доменная система вытеснила таблицы хостов.

Произошло это по следующим причинам:

1) С добавлением новых узлов в сеть росли размеры файла Hosts.txt.

2) Увеличивалось число пользователей, стремившихся получить доступ к компьютеру SRI-NIC, с которого можно было регулярно загружать новые версии этого файла. Следовательно значительно увеличивался сетевой трафик.

3) Отсутствовал контроль за хост-именами, которые администраторы выбирали самостоятельно. Следовательно, возможны совпадения (конфликты) имен и нарушения связи.

Нужен был новый механизм.

Система DNS была разработана в 1983 г. (RFC 882, 883). Документы были обновлены в 1987 г. – RFC 1034, 1035. С тех пор вышло огромное количество RFC, дополняющих стандарт.

DNS (Domain Name System) – Доменная система имен, используемая в Internet.

DNS – служебный протокол прикладного уровня, имеющий архитектуру «клиент-сервер». Основная задача DNS – разрешение доменного имени в IP-адрес.

Система DNS состоит из следующих элементов:

1) Иерархическое доменное пространство имен.
2) Серверы имен доменов.
3) Распознаватели (клиенты, генерирующие запросы для серверов DNS).
4) Зоны.
5) Записи ресурсов.

Иерархическое доменное пространство имен – распределенная БД, рассеянная по многим компьютерам, имеющая иерархическую древовидную структуру.

Самый верхний уровень доменного пространства имен Интернета- корень дерева DNS или корневой домен (обозначается точкой и пустой строкой). Ниже идут домены первого уровня. Затем домены 2-го уровня и т.д..

Иерархия доменных имен аналогична иерархии имен файлов. Домен – эквивалент каталога. Домен может содержать поддомены (субдомены) и хосты.

Домен DNS– множество хостов, объединенных в логическую группу. Домен образуют имена, у которых несколько старших частей совпадают.

Структура доменов отражает не физическое строение сети, а логическое. Компьютеры, входящие в домен, могут иметь совершенно разные IP-адреса, принадлежащие различным сетям и подсетям.

Имя поддомену назначает администратор вышестоящего домена. Т. о. если в каждом домене и поддомене обеспечивается уникальность имен следующего уровня иерархии, то вся система будет состоять из уникальных имен.

Ограничений на количество подуровней в пределах домена нет.

Каждый узел в доменном дереве DNS можно идентифицировать с помощью **полного доменного имени FQDN** (Fully Qualified Domain Name), которое однозначно указывает расположение домена или конечного узла относительно корня доменного дерева. Полное доменное имя состоит из хост-имени данной системы (или типа ресурса) и имен всех родительских доменов, вплоть до корня дерева DNS, разделенных точками.

Перед первой точкой – «личное» имя компьютера или тип ресурса. Далее идет доменная часть – это имя структуры (домена), в которую входит компьютер.

Например: 216-5.povt.fitr.bntu.by. или www.microsoft.com.

Замыкающая точка является стандартным разделителем между меткой домена верхнего уровня и меткой пустой строки, соответствующей корню доменного дерева DNS. (Обычно в браузерах замыкающая точка отбрасывается, однако служба DNS-клиент (DNS Client) добавляет ее в запросах.)

Доменный адрес читается справа налево. Первое слово справа – домен верхнего уровня.

Имена доменов должны следовать международному стандарту ISO 3166.

1) Каждое имя может иметь длину до 63 символов (в некоторых странах до 127).

2) Максимальная длина полного DNS-имени, включая имя хоста и имена всех родительских доменов, не должна превышать 255 символов.
3) Имена доменов и хостов нечувствительны к регистру.

Существует два основных типа доменов верхнего уровня.

■ Организационные (родовые) домены. Имя такого домена указывает основную функцию или род деятельности организаций в DNS-домене. Некоторые организационные домены могут использоваться глобально, другие применяются лишь для организаций в США.

Первоначально родовых доменов было семь:

- com – коммерческие организации;
- edu – образовательные учреждения;
- gov – правительственные учреждения;
- mil – военные организации;
- net – сервисные центры Internet (поставщики услуг);
- org – все остальные организации;
- int – международные организации;

Существуют организационные домены.aero, .biz, .info, .name, .pro и др.

■ Географические домены. Эти домены именуются с использованием кодов страны и региона из двух символов согласно стандарту 3166 Международной организации по стандартизации ISO, например .uk (Великобритания) или .it (Италия).

Частное доменное пространство имен. Помимо доменов верхнего уровня в Интернете организации также могут иметь частное пространство имен — пространство имен DNS на основе набора приватных корневых серверов, которое не зависит от пространства имен DNS в Интернете. В частном пространстве имен можно именовать и создавать собственные корневые серверы и субдомены. Частные имена невозможно видеть или разрешать в Интернете. Примером имени частного домена является имя mycompany.local.

Для работы DNS нужно обеспечить соответствующую конфигурацию DNS-серверов, зон, распознавателей и записей ресурсов.

DNS-сервер представляет собой компьютер с программой DNS-сервера (например, служба DNS-сервера в системе Windows Server или Berkeley Internet Name Domain (BIND) в UNIX).

Для каждого домена создается свой DNS-сервер. Он может хранить информацию для всего домена и всех поддоменов. Однако, такое решение оказывается плохо масштабируемым, т.к. при добавлении новых поддоменов нагрузка может превысить возможности сервера.

Обычно DNS-серверы содержат базу данных с информацией о некоторой части древовидной структуры доменов. Например, только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. При такой организации службы DNS нагрузка по разрешению имен распределяется равномерно между DNS-серверами Internet.

Каждая организация, зарегистрировавшая свой домен, отвечает за свою область пространства имен и может автономно ею управлять. Т. о. нагрузка по администрированию DNS разделена между администраторами сетей.

Для обслуживания корневого домена (.) выделено несколько дублирующих друг друга корневых серверов имен. Их сетевые адреса опубликованы, они обрабатывают миллионы запросов. Все корневые серверы имен принадлежат одному домену root-servers.net и имеют возрастающие хост-имена от a до м.

Корневой домен управляется **ICANN** (Internet Corporation for Assigned Name sand Numbers) -Корпорацией по присвоению имен и номеров в Интернете. Корпорация ICANN координирует назначение идентификаторов, которые должны быть глобально уникальными, для работы в Интернете, включая доменные имена, значения IP-адресов, а

также параметры протоколов и номера портов. Помимо корня домена DNS корпорация ICANN также управляет доменами верхнего уровня.

Корпорация ICANN и другие сообщества именования в Интернете (Network Solutions или Nominent в Великобритании) делегируют домены различным организациям, например Microsoft (microsoft.com) или поставщикам услуг Интернета. Эти организации могут делегировать субдомены другим пользователям.

Сервер, отвечающий за свою часть пространства имен DNS и имеющий свою локально управляемую базу данных (вместо простого кэширования информации с других серверов), является **главным сервером домена**. Он отвечает на запросы об узлах в этом домене. Серверы могут быть главными на одном или нескольких уровнях иерархии доменов. В частности, корневые DNS-серверы в Интернете являются главными лишь для доменных имен верхнего уровня, например, .com.

Каждый DNS-сервер кроме таблицы имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую систему. DNS-серверы, указанные в записях домена высшего уровня, считаются **авторитетными источниками информации** для домена низшего уровня.

Задания на лабораторную работу

Задание 1.

Определить типы адресов локального узла и их значения, используя утилиту ipconfig с ключом /all.

Задание 2.

Разработать консольное приложение, в котором определить и вывести на экран:

1) имя локального хоста, имя домена, полное доменное имя хоста;
2) все сетевые интерфейсы локального хоста (тип, описание, имя);
3) состояние интерфейса (подключен или нет в настоящее время);
4) для каждого интерфейса: физический адрес и размер физического адреса;
   IPv4-адрес, маску, размер IPv4-адреса; размер сетевого префикса;
   IPv6-адрес, размер IPv6-адреса.

Адреса выводить на экран в общепринятой форме записи.

Для получения адресов использовать классы пространства имен System.Net.NetworkInformation (IPGlobalProperties, NetworkInterface, IPInterfaceProperties (свойство UnicastAddresses), PhysicalAddress, DNS и др.).

Сравнить полученные значения адресов с адресами из Задания 1.

Задание 3.

Получить и вывести на экран для заданного пользователем произвольного DNS-имени:

1) IPv4-адреса;
2) IPv6-адреса;
3) Имена-псевдонимы узла (Alias-имена).

Для получения адресов использовать класс Dns пространства имен System.Net.

Задание 4.

Используя специальные поля класса IPAddress, вывести на экран для адресов IPv4 и IPv6:

1) адрес петли обратной связи;
2) широковещательный IP-адрес;

3) адрес, обозначающий все сетевые интерфейсы данного узла.

Контрольные вопросы

1. Какие требования предъявляются к адресу узла сети?
2. Что такое адресное пространство? Приведите пример плоского и иерархического адресного пространства.
3. Какие методы адресации используются в компьютерных сетях? Приведите примеры адресов каждого типа.
4. Как можно классифицировать адреса по количеству адресуемых сетевых интерфейсов?
5. Приведите пример протокола разрешения адресов, использующего централизованный подход, распределенный подход.
6. Что такое локальный адрес? Какая форма записи используется для MAC-адресов? Какой аппаратный адрес используется для широковещательной передачи?
7. Какие системы разрешения имен включают сети Windows Server 2008?
8. Каковы преимущества и недостатки протоколов LLMNR и NetBIOS?
9. Из каких компонентов состоит система DNS?
10. Что представляет собой иерархическое доменное пространство имен? Что такое FQDN?
11. Какие типы доменов верхнего уровня вы знаете? Что такое частное доменное пространство имен?
12. Как доменное имя разрешается в IP-адрес?